6. *Богачкова И. А., Заикин О. С., Кочемазов С. Е. и др.* Задачи поиска коллизий для криптографических хеш-функций семейства MD как варианты задачи о булевой выполнимости // Вычислительные методы и программирование. 2015. Т. 16. С. 61–77.
7. *Отпущенников И. В., Семёнов А. А.* Технология трансляции комбинаторных проблем в булевы уравнения // Прикладная дискретная математика. 2011. № 1. С. 96–115.
8. *Otpuschennikov I., Semenov A., and Kochemazov S.* Transalg: a tool for translating procedural descriptions of discrete functions to SAT // WCSE 2015-IPCE: Proc. 5th Intern. Workshop on Computer Science and Engineering: Information Processing and Control Engineering. 2015. P. 289–294.
9. *Hawkes P., Paddon M., and Rose G.* Musings on the Wang et al. MD5 Collision. IACR Eprint archive. `http://eprint.iacr.org/2004/264`. 2004.
10. *Hirshman G.* Further Musings on the Wang et al. MD5 Collision: Improvements and Corrections on the Work of Hawkes, Paddon, and Rose. Cryptology ePrint Archive, Report 2007/375. 2007.
11. *Stevens M.* Attacks on Hash Functions and Applications. PhD Thesis. Amsterdam: Ipskamp Drukkers, 2012. 258 p.

УДК 519.688 DOI 10.17223/2226308X/9/52

О ВЫЧИСЛЕНИИ ФУНКЦИЙ РОСТА КОНЕЧНЫХ ДВУПОРОЖДЁННЫХ БЕРНСАЙДОВЫХ ГРУПП ПЕРИОДА 5[1]

А. А. Кузнецов, С. С. Карчевский

Пусть $B_0(2,5) = \langle a_1, a_2 \rangle$ — наибольшая конечная двупорождённая бернсайдова группа периода 5, порядок которой равен 5^{34}. Для каждого элемента данной группы существует уникальное коммутаторное представление вида $a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_{34}^{\alpha_{34}}$, где $\alpha_i \in \mathbb{Z}_5$, $i = 1, 2, \ldots, 34$. Здесь a_1 и a_2 — порождающие элементы $B_0(2,5)$; $a_3, \ldots, a_{34}$ — коммутаторы, которые вычисляются рекурсивно через a_1 и a_2. Определим фактор-группу группы $B_0(2,5)$ следующего вида: $B_k = B_0(2,5)/\langle a_{k+1}, \ldots, a_{34} \rangle$. Очевидно, что $|B_k| = 5^k$. В настоящей работе вычислены функции роста B_k относительно порождающих множеств $\{a_1, a_2\}$ и $\{a_1, a_1^{-1}, a_2, a_2^{-1}\}$ для $k = 15$, 16, 17.

Ключевые слова: *функция роста группы, группа Бернсайда.*

Одним из важных инструментов для определения строения группы является изучение её роста относительно фиксированного порождающего множества. Пусть $G = \langle X \rangle$. *Шаром* K_s радиуса s группы G будем называть множество всех её элементов, которые могут быть представлены в виде групповых слов в алфавите X длиной не больше s. Для каждого целого неотрицательного s можно определить функцию роста группы $F(s)$, которая равна числу элементов группы G относительно X, представимых в виде несократимых групповых слов длиной s. Таким образом,

$$F(0) = |K_0| = 1,\ F(s) = |K_s| - |K_{s-1}| \text{ при } s \in \mathbb{N}.$$

Как правило, функцию роста конечной группы представляют в виде таблицы, в которую записывают ненулевые значения $F(s)$.

Пусть $F(s_0) > 0$, но $F(s_0 + 1) = 0$, тогда s_0 является диаметром графа Кэли группы G в алфавите порождающих X, который будем обозначать $D_X(G)$.

[1]Работа поддержана грантом Президента РФ (проект МД-3952.2015.9).

Вычисление функции роста произвольной конечной группы является хотя и разрешимой, но весьма сложной проблемой. Это связано с тем, что в общем случае задача по определению минимального слова элемента группы, как показали С. Ивен и О. Голдрейх [1], является NP-трудной.

Пусть $B_0(2,5) = \langle a_1, a_2 \rangle$ — максимальная конечная двупорождённая бернсайдова группа периода 5, порядок которой равен 5^{34} [2]. Используя систему компьютерной алгебры GAP, нетрудно получить pc-представление (*power commutator presentation*) данной группы [3, 4]. В этом случае каждый элемент $g \in B_0(2,5)$ записывается в виде уникального упорядоченного произведения базисных коммутаторов в определённых степенях:

$$\forall g \in B_0(2,5)\ (g = a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_{34}^{\alpha_{34}},\ \alpha_i \in \mathbb{Z}_5,\ i = 1, 2, \ldots, 34).$$

Здесь коммутаторы a_1 и a_2 являются порождающими элементами группы, а последующие — $a_3, \ldots, a_{34}$ — определяются рекурсивно через a_1 и a_2 [2].

Обозначим через B_k фактор-группу группы $B_0(2,5)$ следующего вида:

$$B_k = B_0(2,5)/\langle a_{k+1}, \ldots, a_{34} \rangle.$$

Очевидно, что $|B_k| = 5^k$ и $\forall g \in B_k\ (g = a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_k^{\alpha_k})$.

К. А. Филипповым в [5] вычислена функция роста группы B_{14} в алфавите $A_2 = \{a_1, a_2\}$. Аналогичная задача для симметричного порождающего множества $A_4 = \{a_1, a_1^{-1}, a_2, a_2^{-1}\}$ решена Ч. Симсом [6]. В обоих случаях решение было получено при помощи длительных компьютерных вычислений.

Одной из причин интереса исследователей к функциям роста B_k является то, что получаемая информация может оказаться полезной при решении открытой проблемы о конечности $B(2,5)$ — свободной двупорождённой бернсайдовой группы периода 5.

Дальнейшее изучение функций роста групп B_k для $k > 14$ сталкивается с серьёзными вычислительными трудностями ввиду их больших порядков.

Настоящая работа посвящена разработке эффективного алгоритма для вычисления функций роста указанных групп, который бы дал возможность преодолеть существующий барьер. За основу взят алгоритм, описанный в [7]. Для быстрого умножения элементов группы использовались полиномы Холла, полученные в [8]. Введён новый метод упорядочивания элементов, который позволил значительно повысить быстродействие. Модифицированный алгоритм реализован на 4-процессорном компьютере (на каждом по 16 ядер) с общей памятью объемом 256 Гб. В результате вычислены функции роста групп B_k для $k = 15$, 16 и 17.

В таблице приведены значения диаметров графов Кэли групп B_k, полученные в настоящей работе, а также уже известные; на рис. 1 и 2 приведены графики роста функций B_k.

k	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$D_{A_2}(B_k)$	8	10	13	20	20	25	30	31	32	35	40	40	45	46	50	55
$D_{A_4}(B_k)$	4	6	9	10	13	15	19	20	20	24	26	28	30	30	33	34

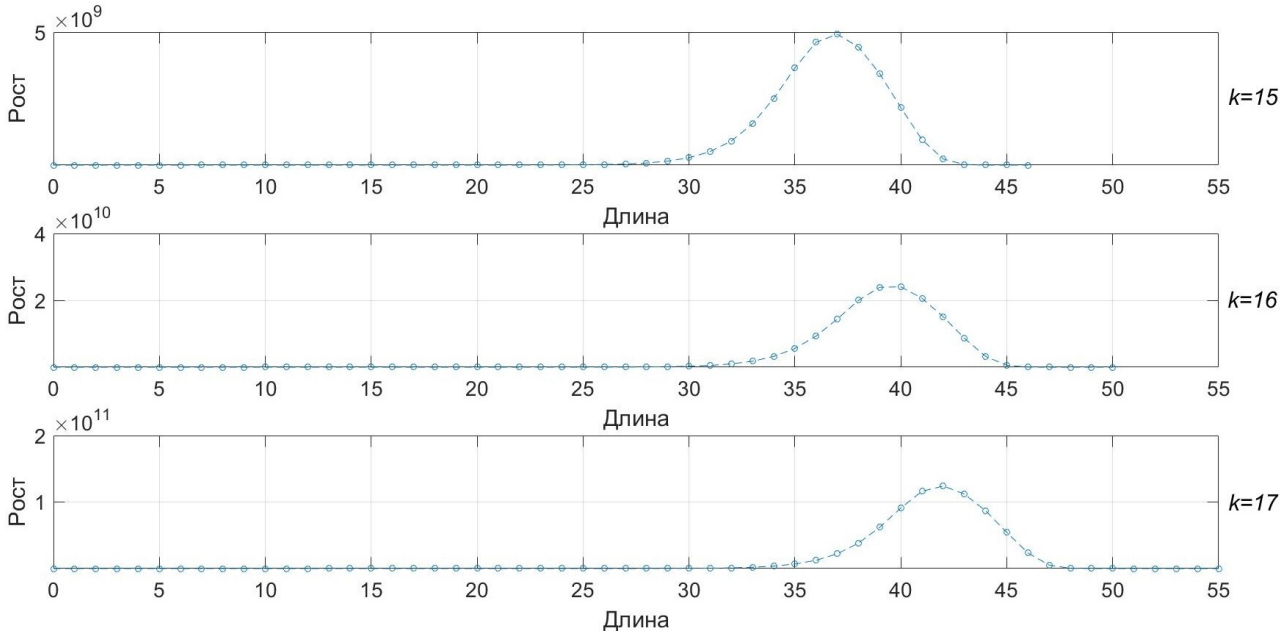

Рис. 1. Графики функций роста групп B_k в алфавите A_2

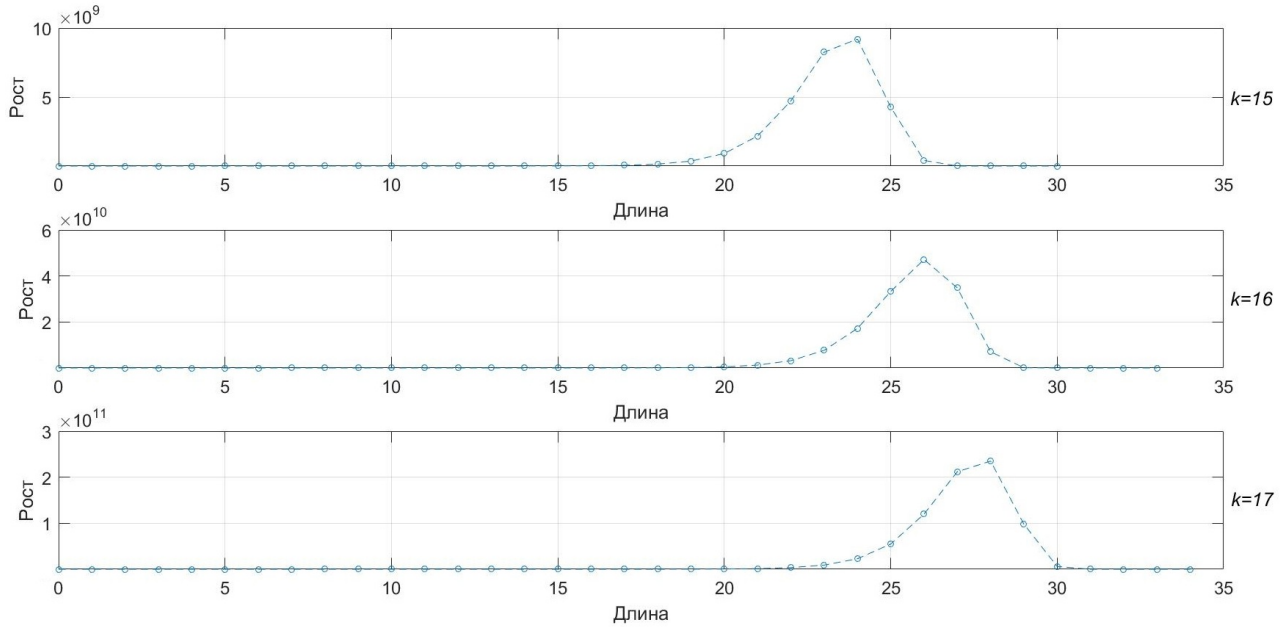

Рис. 2. Графики функций роста групп B_k в алфавите A_4

ЛИТЕРАТУРА

1. *Even S. and Goldreich O.* The minimum length generator sequence is NP-hard // J. Algorithms. 1981. V. 2. No. 3. P. 311–313.
2. *Havas G., Wall G., and Wamsley J.* The two generator restricted Burnside group of exponent five // Bull. Austral. Math. Soc. 1974. No. 10. P. 459–470.
3. *Sims C.* Computation with Finitely Presented Groups. Cambridge: Cambridge University Press, 1994. 628 p.
4. *Holt D., Eick B., and O'Brien E.* Handbook of Computational Group Theory. Boca Raton: Chapman & Hall/CRC Press, 2005. 514 p.

5. *Филиппов К. А.* О диаметре Кэли одной подгруппы группы $B_0(2,5)$ // Вестник СибГАУ. 2012. Т. 41. № 1. С. 234–236.
6. *Sims C.* Fast multiplication and growth in groups // Proc. 1998 Intern. Symp. on Symbolic and Algebraic Computation. N. Y., USA, 1998. P. 165–170.
7. *Кузнецова А. С., Кузнецов А. А., Сафонов К. В.* Параллельный алгоритм вычисления функций роста в конечных двупорождённых группах периода 5 // Прикладная дискретная математика. Приложение. 2013. № 6. С. 119–121.
8. *Кузнецов А. А., Кузнецова А. С.* Быстрое умножение элементов в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2013. № 1. С. 110–116.